# Safeguard Computer Security Evaluation Matrix (SCSEM)

# IBM RACF

# Release IV

# 7-Dec-07


**Tester:** *Insert Tester Name*
**Date:** *Insert Date(s) Testing Occured*
**Location:** *Insert Location testing was conducted*
**Agency POC(s):** *Insert Agency interviewee(s) names*

| Test ID | NIST ID | Test Objective | Test Steps | Expected Results | Actual Results | Pass/ Fail | Comments/ Supporting Evidence |
|---|---|---|---|---|---|---|---|
| 1 | AC-2 | UserIDs defined in SYS1.UADS are limited to emergency and disaster recovery systems personnel. | Consult with RACF Security Administrator and verify that UserIDs defined the TSO User Attribute Dataset (SYS1.UADS) are restricted to emergency and disaster recovery systems personnel. | UserIDs defined the TSO User Attribute Dataset (SYS1.UADS) are restricted to emergency and disaster recovery systems personnel. | | | |
| 2 | AC-2, IA-5 | The vendor-supplied account (IBMUSER) has been revoked after successful installation of RACF security database. | Review DSMON “Selected User Attribute Report”<br>Verify IBMUSER is revoked. | IBMUSER is revoked. | | | |
| 3 | AC-3, CM-3 | Real Data Set Names option is active. | Review the SETROPTS list and verify that the Real Data Set Names option is in effect | Real Data Set Names option is in effect | | | |
| 4 | AC-3, CM-3 | The RACF Exits Report (RACEXT) should state “No RACF EXITS ARE ACTIVE,” or all RACF exits active on a system must be reviewed and verified for authorized changes. | Consult with the system administrator that the DSMON RACF Exits Report should state “No RACF EXITS ARE ACTIVE,” or all RACF exits active on a system must be reviewed and verified for authorized changes. | The RACF Exits Report states “No RACF EXITS ARE ACTIVE,” or all RACF exits active on a system must be reviewed and verified for authorized changes. | | | |
| 5 | AC-3, CM-3 | SYS1 is the highest level (Level 1) group for any RACF implementation. | Review the DSMON RACF Group Tree Report and verify: (1) SYS1 is the Level 1 Group of the tree hierarchy; and (2) IBMUSER owns the SYS1 group. | (1) SYS1 is the Level 1 Group of the tree hierarchy; and (2) IBMUSER owns the SYS1 group. | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 6 | AC-3, CM-3 | IBMUSER owns SYS1. | Review the DSMON RACF Group Tree Report and ensure no USERID is the owner of a group, except IBMUSER -- who owns SYS1. | No USERID is the owner of a group, except IBMUSER | | | |
| 7 | AC-3, CM-3 | The SECURITY (Level 2) group is directly subordinate to SYS1. | Review the DSMON RACF Group Tree Report and verify that the SECURITY (Level 2) group is owned by SYS1. | The SECURITY (Level 2) group is owned by SYS1 | | | |
| 8 | AC-3, CM-3 | The PRIVILEGED attribute is set to “NO” for system-started tasks, procedures, and programs. | 1. Review the DSMON RACF Started Procedures Table Report to identify system started tasks, procedures, and programs with the PRIVILEGED attribute – These programs can bypass RACF security checks and auditing controls.<br>2. Ensure the PRIVILEGED attribute is set to “NO” for the system started tasks, except for critical started procedures that should be defined as TRUSTED on IBM’s recommendation (e.g., NET, JESA, JES2)<br>3. Ensure the generic entry “*” is not assigned the PRIVILEGED or TRUSTED attribute. | PRIVILEGED attribute is set to “NO” for the system started tasks, except for critical started procedures that should be defined as TRUSTED and the generic entry “*” is not assigned the PRIVILEGED or TRUSTED attribute | | | |
| 9 | AC-3, CM-3 | CATALOGUED DATA SETS ONLY is not in effect. | Review the SETROPTS list to verify the CATALOGUED DATA SETS ONLY option is disabled. | CATALOGUED DATA SETS ONLY IS NOT IN EFFECT. | | | |
| 10 | AC-3, CM-3 | ENHANCED GENERIC NAMING is not active. | Review the SETROPTS list configuration for ENHANCED GENERIC NAMING. | ENHANCED GENERIC NAMING IS NOT IN EFFECT | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 11 | AC-3, CM-3 | PROTECT-ALL FAIL mode option is active. | Review the SETROPTS list and verify Protect-All Fail security parameter is activated to ensure that datasets are RACF-protected. | PROTECT-ALL IS ACTIVE, CURRENT OPTIONS: PROTECT-ALL FAIL OPTION IS IN EFFECT | | | |
| 12 | AC-3, CM-3 | TAPE DATA SET PROTECTION is active. | Review the SETROPTS list and verify for the Tape Dataset Protection security parameter is activated to ensure that tape datasets are RACF-protected. | TAPE DATA SET PROTECTION IS ACTIVE | | | |
| 13 | AC-3, CM-3 | The SETROPTS ATTRIBUTES operand is set to WHEN (PROGRAM). | Review the SETROPTS list to ensure WHEN (PROGRAM) is active.<br><br>WHEN (PROGRAM) ensures RACF control is active for program load modules and program-accessed datasets through explicit profile definitions in the PROGRAM class. | WHEN (PROGRAM) is active. | | | |
| 14 | AC-3, CM-3 | GENERIC PROFILE CLASSES is turned on for active classes. | Obtain SETROPTS list and compare the entries of the Generic Profile Classes with the entries the Active Classes. | At a minimum, generic profile classes should be turned on the following active resource classes: DATASET, TERMINAL, CICS Resources, TSOPROC, ACCTNUM, TSOAUTH, TAPEVOL, DASDVOL, JESSPOOL, JESSJOBS. | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 15 | AC-3, CM-3 | GENERIC COMMAND CLASSES is turned on for active classes. | Obtain SETROPTS list and compare the entries of the Generic Command Classes with the entries the Active Classes. | At a minimum, generic command classes should be turned on the following active resource classes: DATASET, TERMINAL, CICS Resources, TSOPROC, ACCTNUM, TSOAUTH, TAPEVOL, DASDVOL, JESSPOOL, JESSJOBS. | | | |
| 16 | AC-3, CM-3 | All APF library programs reside on specified volumes, and APF library programs are restricted with a UACC of NONE or READ (where appropriate). | Procedures:<br>1. Consult with the RACF security administrator about APF library documentation.<br>2. Use the DSMON RACF Selected Data Sets Report to list APF libraries that are not resident on specified volumes.<br>3. Use the DSMON RACF Selected Data Sets Report to the UACC for APF libraries. | All APF library programs reside on specified volumes, and APF library programs are restricted with a UACC of NONE or READ (where appropriate). | | | |
| 17 | AC-3, CP-2 | Primary and backup RACF data sets are on different volumes and marked ‘unmovable.’ | Consult with the computer operation manager regarding the handling of RACF primary and backup data sets. | Primary and backup RACF data sets are on different volumes and marked ‘unmovable.’ | | | |
| 18 | AC-3, CP-4 | Tapes cannot be used until the tape management system expires the volume and all DSNs on the volume, or to a reasonable limit. | Review the SETROPTS list (only applicable if this is not handled by a tape management such as CA-1) | SECURITY RETENTION PERIOD IN EFFECT IS 99999 DAYS | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 19 | AC-4, SC-9, SC-23 | Checks to see if the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures | Interview the SA or ISSO to determine if all connections to the Mainframe are via *SSH or *Other communications methods using tunneling via or equivalent FIPS encryption. | The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures | | | |
| 20 | AC-5 | The SPECIAL attribute is restricted to IS personnel routinely tasked with performing RACF security administration of the system. | 1. Review the DSMON RACF Selected User Attribute Report to identify User IDs with the system SPECIAL attribute.<br>2. Interview the Primary RACF Security Administrator and determine the appropriateness of User IDs with the system SPECIAL attribute. | The SPECIAL attribute is restricted to IS personnel routinely tasked with performing RACF security administration of the system. | | | |
| 21 | AC-5 | The OPERATIONS attribute is restricted to systems personnel routinely tasked with performing storage management system (SMS) functions. | Review the DSMON RACF Selected User Attribute Report to identify User IDs with the system OPERATIONS attribute. Interview the Primary RACF Security Administrator and determine the appropriateness of User IDs with the system OPERATIONS attribute. | The OPERATIONS attribute is restricted to systems personnel routinely tasked with performing storage management system (SMS) functions. | | | |
| 22 | AC-5 | The AUDITOR attribute is restricted to IS personnel routinely tasked with performing RACF security administrative/RACF security auditing functions. | Review the DSMON RACF Selected User Attribute Report to identify User IDs with the system AUDITOR attribute. Interview the Primary RACF Security Administrator and determine the appropriateness of User IDs with the system AUDITOR attribute. | The AUDITOR attribute is restricted to IS personnel routinely tasked with performing RACF security administrative/RACF security auditing functions. | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 23 | AC-6 | All TSO resources are active and defined to RACF. | 1. Review the CLASSACT operand (ACTIVE CLASSES) of the SETROPTS list to verify that TSO resource classes (i.e., TSOPROC, ACCTNUM, PERFGRP, and TSOAUTH) are active in the Class Descriptor Table (CDT).<br><br>2. List TSO users defined to SYS1.UADS dataset. Verify users are defined to RACF. Use RACF LU command (LISTUSER) to list each TSO user's RACF user profile. | TSO resource classes (i.e., TSOPROC, ACCTNUM, PERFGRP, and TSOAUTH) are active and TSO users are defined to RACF | | | |
| 24 | AC-6 | Access control procedures governing the use of RVARY commands are adequate. | Verify written procedures are established and disseminated to ensure: (1) Use of RVARY commands are restricted to authorized personnel and approved by appropriate systems management personnel; (2) knowledge of RVARY passwords are restricted to authorized personnel; (3) Passwords for RVARY commands are changed regularly; and (4) Use of RVARY commands are monitored regularly. | (1) Use of RVARY commands are restricted to authorized personnel and approved by appropriate systems management personnel; (2) knowledge of RVARY passwords are restricted to authorized personnel; (3) Passwords for RVARY commands are changed regularly; and (4) Use of RVARY commands are monitored regularly. | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 25 | AC-6 | Resources are active and defined to RACF. | Obtain SETROPTS list and review the CLASSACT Option (Active Classes). | Verify that the following IBM-supplied resource classes in the Class Descriptor Table (CDT) are activated: DATASET, USER GROUP, DASDVOL, TAPEVOL, TERMINAL, APPL, CICS resource group profiles, TSOPROC, ACCTUM, TSOAUTH, DSNR | | | |
| 26 | AC-6 | Bypass Label Processing (BLP) is restricted to appropriate systems personnel. | Obtain access control list (LIST) for the DITTO.TAPE.BLP or ICHBLP resource within the FACILITY class and verify appropriateness of users with access to the tape BLP resource | Only appropriate users have access to BLP. | | | |
| 27 | AC-6 | Entries residing in the MVS Program Properties Table (PPT) are configured in accordance IBM recommendations. | Review the DSMON Program Properties Table Report and identify programs that: (1) bypass RACF password protection; and (2) reside in a system key. | Ensure the aforementioned programs are configured in accordance with IBM-supplied recommendations. | | | |
| 28 | AC-6 | Users are not assigned the ALTER, CONTROL or UPDATE access authority to the SMF audit files (e.g. SYS1.MAN*). | Obtain access control list (ACL) for the SYS1.MAN datasets from the RACF Security Administrator. NOTE: Preferably, this list should be generated in the presence of the system evaluator. The following syntax should be used to generate the aforementioned ACL: LD DS ('SYS1.MAN*') GN AUTH | Users are not assigned the ALTER, CONTROL or UPDATE access authority to the SMF audit files (e.g. SYS1.MAN*). | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 29 | AC-6 | The ALTER and UPDATE access authority for MVS operating system datasets is restricted to appropriate systems personnel (e.g. ALTER restricted to OS390 system programmers) | Obtain access control lists (ACLs) for the APF libraries/datasets (listed below in parenthesis) from the RACF Security Administrator. NOTE: Preferably, this list should be generated in the presence of the system evaluator.<br>The following syntax should be used to generate the aforementioned ACLs:<br>LD DS('SYS1.NUCLEUS') GN AUTH<br>LD DS('SYS1.LINKLIB') GN AUTH<br>LD DS ('SYS1.LPALIB') GN AUTH<br>LD DS ('SYS1.MIGLIB') GN AUTH<br>LD DS ('SYS1.PARMLIB') GN AUTH<br>LD DS ('SYS1.SVCLIB') GN AUTH<br>LD DS ('SYS1.UADS') GN AUTH<br>LD DS ('SYS1.VTAMLIB') GN AUTH<br>LD DS ('SYS1.VTAMLST') GN AUTH | The ALTER and UPDATE access authority for MVS operating system datasets is restricted to appropriate systems personnel (e.g. ALTER restricted to OS390 system programmers) | | | |
| 30 | AC-6 | Review FTI dataset access control list to determine if access is appropriate. | Consult with system administrator to determine potential access control deficiencies.<br><br>Ensure users with OPERATIONS are prohibited from accessing FTI datasets (entry on ACL of NONE). Ensure UACC is set to NONE for FTI datasets. | Users with OPERATIONS are prohibited from accessing FTI datasets (entry on ACL of NONE). UACC is set to NONE for FTI datasets. | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 31 | AC-6 | UACC is set to NONE for applicable RACF Global access authorization. | Review the RACF DSMON Global Access Table Report with the RACF security administrator to verify if each UACC is set to NONE for applicable RACF Global access authorizations. | To facilitate system performance and ensure data security, specific DSNs are allowed UACC access at the READ, UPDATE, or ALTER, access level. For sensitive system DSNs, the RACF Global Access must be set to UACC=NONE. For example, the following SYS1 DSNs are allowed UACC=READ:<br><br>SYS1.BROADCAST*.**<br>SYS1.COBLIB*.**<br>SYS1.IRSMACRO*.**<br>SYS1.LINKLIB*.**<br>SYS1.MACLIB*.** | | | |
| 32 | AC-7 | User accounts are revoked after three (3) consecutive, unsuccessful login attempts. | Review SETROPTS list and verify the following configuration for revoking user accounts: | AFTER 3 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS, A USERID WILL BE REVOKED. | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 33 | AC-8 | All computer systems must have an IRS-approved screen-warning banner, which outlines the nature and sensitivity of information processed on the system and the consequences / penalties for misuse. | Review the logon warning banner for information consistent with IRS-approved documentation<br>Sample IRS approved banner:<br>UNAUTHORIZED ACCESS TO THIS UNITED STATES GOVERNMENT COMPUTER SYSTEM AND SOFTWARE IS PROHIBITED BY PUBLIC LAW 99-474, TITLE 18, UNITED STATES CODE. PUBLIC LAW 99-474 AND CHAPTER XXI, SECTION 1030 STATES THAT Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, obtains, alters, damages, destroys, or discloses information, or prevents authorized use of (data or a computer owned by or operated for) the Government of the United States, shall be punished by a fine under this title or imprisonment for not more than 10 years, or both. All activities on this system may be recorded and monitored. Individuals using this system expressly consent to such monitoring. Evidence of possible misconduct or abuse may be provided to appropriate officials. | The IRS approved login banner is displayed prior to a login attempt.<br><br>If the device can only support a short banner, the contents of the banner should be:<br>WARNING! US GOVERNMENT SYSTEM. Unauthorized access prohibited by Public Law 99-474 "The Computer Fraud and Abuse Act of 1986". Use of this system constitutes CONSENT TO MONITORING AT ALL TIMES and is not subject to ANY expectation of privacy. | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 34 | AC-11 | All dial-up access to the IBM 9762 R75 is protected with approved devices or techniques that provide explicit identification and authentication and audit trails. | Consult with the system administrator and verify that dial-up access is controlled through security measures. | Dial-up access is not present or controlled through security measures. | | | |
| 35 | AC-11, AC-12, SC-10 | Determine if automatic session termination applies to local and remote sessions. | The SA will configure systems to log out<br>interactive processes (i.e., terminal sessions, ssh sessions, etc.,) after 15 minutes of inactivity<br>or ensure a password protected screen lock mechanism is used and is set to lock the screen<br>after 15 minutes of inactivity. | Systems are configured to log out of interactive processes (i.e., terminal sessions, ssh sessions, etc.,) after 15 minutes of inactivity<br>or ensure a password protected screen lock mechanism is used and is set to lock the screen<br>after 15 minutes of inactivity. | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 36 | AC-13, AU-1, AU-6 | Checks to see if audit trails and/or system logs are reviewed on a daily basis(or an interval stated in local policy). | Ask the SA/ISSO if audit files are reviewed daily (or as stated by a policy interval) If the audit files are not reviewed daily (or according to local policy), then this is a finding. | Audit trails and/or system logs are reviewed on a daily basis for:<br>- Excessive logon attempt failures by single or multiple users<br>- Logons at unusual/non-duty hours<br>- Failed attempts to access restricted system or data files indicating a possible pattern of deliberate browsing<br>- Unusual or unauthorized activity by System Administrators<br>- Command-line activity by a user that should not have that capability<br>- System failures or errors<br>- Unusual or suspicious patterns of activity | | | |
| 37 | AC-14, AC-17, SC-2 | Checks to see if services that allow interaction without authentication or via anonymous authentication are documented, justified to the ISSO, and are properly secured and segregated from other systems that contain services that explicitly require authentication and identity verification. | Determine if the organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives. Examples are access to public facing government service websites such as www.firstgov.gov. | Services that allow interaction without authentication or via anonymous authentication are documented, justified to the ISSO, and are properly secured and segregated from other systems that contain services that explicitly require authentication and identity verification. | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 38 | AC-17 | Check to see that Virtual Private Network (VPN) (or similar technology providing protection (e.g., end-to-end encryption)) is being used when remotely accessing the system. | Interview the system administrator to determine if remote access is:<br>i. monitored on a periodic basis in accordance with organization policy<br>ii. authorized and restricted to users with an operational need for access<br>iii. restricted to only allow privileged access based on compelling operational needs.<br>iv. authenticated and protected with a VPN solution when accessing personally identifiable information. | i. Logs or real-time monitoring software is running that indicates remote access is monitored.<br>ii. The remote access solution requires users to authenticate when connecting remotely.<br>iii. Access to remote maintenance ports are only be available to explicitly identified personnel. Employees must submit a request to their supervisors prior to being granted remote access. iv. VPN or other secure solution is utilized. | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 39 | AU-2, AU-3, AU-8, AU-9 | Auditing is configured to capture unsuccessful security-relevant events (e.g., logon failure, user violations). Audit events include the original of request (e.g., terminal ID) for logon, logoff, password change, and user system activities. Each audit event trails the user and information relevant to the event (e.g., date and time of the event, user, type of event, file name and the success or failure of the event). The audit record shall include the file name of the file related event. | Request and review Security Administrator to generate audit and security reports by batch:<br>-System Users with SPECIAL Attribute Report<br>-System Users with OPERATION Attribute Report<br>-RACF User Violation Report. | 1. Each audit event trails the user and information relevant to the event (e.g., date and time of the event, user, type of event, file name and the success or failure of the event). The audit report records the date and time of the security events, the user, and the type of event/commands performed by privileged users (e.g., ADDUSER, ALTUSER, and DELUSER USERID). 2. The violation report records audit events, which include the original of request (e.g., terminal ID) for logon, logoff, password change, and user system activities. 3. The RACF violation reports distributed to and reviewed by the RACF Security Administrator / Security Auditor he violation report records audit events which include the original of request (e.g., terminal ID) for logon, logoff, password change, and user system activities. | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 40 | AU-2 | The STATISTICS parameter in the SETROPTS list must turned on for all active resource classes defined. | Verify the SETROPTS STATISTICS parameter setting for auditing on all active resource classes defined for FTI resources that have unique security concerns (e.g., sensitive, critical resources). | STATISTICS is turned on. | | | |
| 41 | AU-2 | The SETROPTS LOGOPTIONS command is set to DEFAULT. | Verify the configuration for the SETROPTS LOGOPTIONS “DEFAULT’ CLASSES parameter. | The SETROPTS LOGOPTIONS command is set to DEFAULT. | | | |
| 42 | AU-2 | The ATTRIBUTES operand in the SETROPTS list must be set to INITSTATS, SAUDIT, OPERAUDIT, CMDVIOL. | Verify the system controls as configured for the ATTRIBUTES parameter of the SETROPTS list is properly defined. | The ATTRIBUTES parameter in the SETROPTS list is set to INITSTATS, SAUDIT, OPERAUDIT, CMDVIOL. | | | |
| 43 | AU-2 | All active resource classes shall have AUDIT feature turned on. | 1. Identify all active resource classes as defined to the ACTIVE CLASSES parameter of the SETROPTS list.<br><br>2. Compare the list with all entries defined to the AUDIT CLASSES parameter of the SETROPTS list. | All active resource classes shall have AUDIT feature turned on. Entries are identical on both lists. | | | |
| 44 | AU-2 | The system activities of personnel assigned system-level authorities must be audited at all times by activating SAUDIT, OPERAUDIT, and CMDVIOL. | Verify the SETROPTS ATTRIBUTES setting for auditing on privileged system users who are assigned System SPECIAL, OPERATIONS, and AUDITOR attributes. | Verify that comprehensive policies and procedures are established to define auditing requirements. | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 45 | AU-4, AU-11 | Check to see if the organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded. | Interview ISSO or SA and ask if log storage is sufficient to meet IRS logging and retention requirements. | Sufficient storage is available to meet IRS logging and retention policies. | | | |
| 46 | AU-5 | Checks to see if the organization responds to audit processing failures. | Interview the system administrator to verify the following actions occur in the event of an audit failure or storage capacity being reached:<br>1. In the event the audit log becomes full, a scheduled job shall be executed to archive the log to a secure location on the server for the Mainframe; it shall include DASD or other media<br>2. In the event the security event log is manually cleared by the system administrator, this should be recorded as an auditable event for future analysis.<br>3. Security event logging should be configured to capture the clearing of the security event log itself as an auditable event. | 1. A scheduled job is executed to archive the log to a secure location on the server for the Mainframe; it shall include DASD or other media<br>2. Security event logs manually cleared by the system administrator is recorded as an auditable event for future analysis.<br>3. Security event logging is configured to capture the clearing of the security event log itself as an auditable event. | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 47 | AU-9 | Checks to see if the organization protects audit information. | Logon to TSO as a standard TSO end-user and attempt to generate and view any of the following mainframe audit reports via the Data Security Monitor (DSMON) facility:<br>- System and RACF Identification Report (SYSTEM)<br>- Program Properties Table (PPT) Entries Report (SYSPPT)<br>- RACF Authorized Caller Table Entries Report (RACAUT)<br>- RACF Exits Report (RACEXT)<br>- RACF Class Descriptor Table Entries and Status Report (RACCDT)<br>- RACF Started Class and Started Task Table Entries Report (RACSPT)<br>- APF Library Protection Report (SYSAPF)<br>- Linklist Library Protection Report (SYSLNK)<br>- System Dataset Protection Report (SYSSDS)<br>- Catalog Dataset Protection Report (SYSCAT)<br>- RACF Database Protection Report (RACDST)<br>- RACF Global Access Table Entries Report (RACGAC)<br>- RACF Group Tree Report (RACGRP)<br>- RACF User Attributes Report (RACUSR) | A standard TSO user does not have the AUDIT attribute to perform system audit functions. A standard end-user is not allowed to use the TSO facility. Only RACF Security Administrators have access to these audit reports. | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 48 | IA-2 | UserIDs are provided for all Network Job Entry (NJE) nodes. | Review the SETROPTS list to verify that all users submitting batch jobs through NJE processes will require a UserID. | USER-ID FOR JES NJEUSERID IS: ????????<br>(The default USERID is for inbound jobs and protects jobs residing on spool).<br>USER-ID FOR JES UNDEFINED USER IS: ++++++++<br>(The JES undefined USERID prevents undefined users from accessing RACF-protected resources on the system). | | | |
| 49 | IA-2 | All started tasks have a RACF UserID associated with them. | Review the DSMON RACF Started Procedures Table to verify that all started tasks have a RACF USERID associated with them, such that all access authorizations will be dependent on the associated USERID protected by RACF. | A generic catch all profile of '**' is coded to the last entry in the STARTED class and/or the last entry in the ICHRIN03 SPT is marked with an asterisk ('*'). | | | |
| 50 | IA-2, IA-4 | Each USERID is unique and is consistent with the naming conventions of the facility. | Review the RACF Selected User Attribute Report to verify that each USERID established on the RACF database is unique and is consistent with the entity's naming-conventions policy. | Each USERID established on the RACF database is unique and is consistent with the entity's naming-conventions policy. | | | |
| 51 | IA-2 | Passwords must be 8 alphanumeric characters, with a minimum of one (1) numeric character. | Review PASSWORD PROCESSING OPTIONS of the SETROPTS list and verify configuration for the INSTALLATION SYNTAX RULES. | RULE 1 LENGTH (8:8) LLLLLL | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 52 | IA-3 | The RVARY passwords for the Switch and Status functions are set to “Installation Defined”. | Review the INSTALLATION DEFINED RVARY PASSWORD options of the SETROPTS list to verify the RVARY passwords are not set to default. | Installation defined rvary password is in effect for the switch function.<br>Installation defined rvary password is in effect for the status function. | | | |
| 53 | IA-3 | Users are forced to change passwords at a maximum of 90 days. | Review the PASSWORD PROCESSING OPTIONS of the SETROPTS list and verify the configuration for Password Change Interval. | PASSWORD CHANGE INTERVAL IS 90 DAYS | | | |
| 54 | IA-3 | User accounts that are inactive for a period of 90 days will be revoked | Review the SETROPTS list to verify the configuration for revoking inactive user accounts. | INACTIVE USERIDS ARE BEING AUTOMATICALLY REVOKED AFTER 90 DAYS. | | | |
| 55 | IA-3 | Password history shall be maintained for a minimum of six (6) generations. | Review the PASSWORD PROCESSING OPTIONS of the SETROPTS list and verify the configuration for password history. | 6 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED | | | |
| 56 | IA-3 | Users are notified to change their passwords before the password change interval is enforced. | Review the PASSWORD PROCESSING OPTIONS of the SETROPTS list to verify the configuration for Password Expiration Warning. | PASSWORD EXPIRATION WARNING LEVEL IS XX DAYS. (XX denotes a value between 5-14.) | | | |
| 57 | IA-3, CM-3 | JES-BATCHALLRACF option is active. | Review SETROPTS list to verify the configuration for the Job Entry System (JES) remote access parameters. | JES-BATCHALLRACF OPTION IS ACTIVE<br>(This option forces users to identify themselves to RACF). | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 58 | IA-3, CM-3 | JES-XBMALLRACF option is active. | 1. Review SETROPTS list to verify the configuration for the Job Entry System (JES) remote access parameters: JES-XBMALLRACF OPTION IS ACTIVE (This option is required if XBATCH is setup in JES). 2. Verify with RACF Security Administrator that UserIDs and passwords are not embedded in job cards when submitting batch jobs. | JES-XBMALLRACF OPTION IS ACTIVE and UserIDs and passwords are not embedded in job cards when submitting batch jobs. | | | |
| 59 | IA-6 | Check to see if the feedback from the information system provides information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information. | Interview ISSO or SA and ask if any applications or services display the user or service account password during input or after authentication. | The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 60 | SC-2 | Check to see if the information system separates user functionality (including user interface services) from information system management functionality. | Interview the SA or ISSO and ask if the information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate. | The information system separates user functionality (including user interface services) from information system management functionality. | | | |
| 61 | SC-2, SC-4 | ERASE-ON-SCRATCH is turned on the ERASE indicator is established in the FTI dataset profile. | Review the SETROPTS list and verify that the ERASE-ON-SCRATCH (EOS) operand is specified without any sub-operands (e.g. ALL)<br>Identify the FTI data sets and review the results of the following command that will list the ERASE option configured for the data set. | ERASE-ON-SCRATCH IS ACTIVE<br>BY SECURITY LEVEL IS INACTIVE<br>LD DATASET(‘data set name’) ALL<br>The ERASE indicator is set to YES. | | | |
| 62 | SC-5 | Denial of service | Examine information system design documents and procedures addressing denial of service protection to verify the information system protects against or limits the effects of denial of service attacks. | the information system protects against or limits the effects of denial of service attacks. | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 63 | IA-7, SC-13 | Checks to see that when information requires cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. | Interview the SA or ISSO to determine if FIPS 140-2 encryption is used on items requiring the use of cryptography for protection. | For information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with FIPS-140-2, applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. | | | |

## IRS Safeguard SCSEM Legend

Test Case Tab: Execute the test cases and document the results to complete the IRS Safeguard Computer Security review. Reviewer is required to complete the following columns: Actual Results, Comments/Supporting Evidence.

| | |
|---|---|
| **Test ID** | Identification number of SCSEM test case |
| **NIST ID** | NIST 800-53/PUB 1075 Control Identifier |
| **Test Objective** | Objective of test procedure. |
| **Test Steps** | Detailed test procedures to follow for test execution. |
| **Expected Results** | The expected outcome of the test step execution that would result in a Pass. |
| **Actual Results** | The actual outcome of the test step execution, i.e., the actual configuration setting observed. |
| **Pass/Fail** | Reviewer to indicate if the test case pass, failed or is not applicable. |
| **Comments / Supporting Evidence** | Reviewer to include any supporting evidence to confirm if the test case passed., failed on not applicable As evidence, provide the following information for the following assessment methods:<br>1. Interview - Name and title of the person providing information. Also provide the date when the information is provided.<br>2. Examination - Provide the name, title, and date of the document referenced as the evidence. Also provide section number where the pertinent information is resident within the document (if possible).<br><br>Ensure all supporting evidence to verify the test case passed or failed. If the control is marked as NA, then provide appropriate justification as to why the control is considered NA. |